Enhancing Power-Side-Channel-Attack Resistance via a Security-Aware Integrated Voltage Regulator

M. Kar[1], A. Singh[1], S. Mathew[2], A. Rajan[2], V. De[2] and S. Mukhopadhyay[1]
[1]School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA
[2]Intel, Hillsboro, OR

Power side channel attacks (PSCA) are major threats to the security of crypto engines across different platforms, from the servers all the way to the IoTs. Integrated voltage regulators, which have become an integral part of power delivery architecture for high performance digital processors, can be exploited to enhance PSCA resistance. We demonstrate improved PSCA resistance offered by an on-die all-digital high-frequency fully integrated inductive voltage regulator (IVR) in 130nm CMOS for a standard (unprotected) 128-bit Advanced Encryption Standard (AES) core designed in static CMOS logic. The IVR features a configurable digital PID controller, a digital discontinuous conduction mode (DCM) controller, and a loop randomization (LR) block, all of which are utilized to enhance PSCA resistance with minimal power/performance/area overheads while maintaining adequate local voltage regulation and transient performance. IVR reduces information leakage and increases PSCA resistance by introducing three different transformations on the current signatures of the crypto engine before it is measured by the attacker at the IVR's supply. The large signal transformation introduces pulsating pattern at the IVR input, small signal transformation introduces frequency dependent distortion, and the IVR switching clock makes alignment of the captured signals difficult. The standalone AES was attacked in 5000 measurements, however the correlation power analysis with 100000 measurements remains unsuccessful at the input of the IVR. However test-vector leakage assessment (TVLA) shows signs of leakage at the IVR input. The leakage from the IVR input reduces when the discontinuous conduction mode is activated in the IVR. LR is activated to introduce randomness in the loop, changing all three transformation through the IVR. Both CPA and TVLA tests were unsuccessful at the IVR input with LR activated. The paper was published at **International Solid State Circuits Conference (ISSCC), 2017** and selected as the highlighted paper of the security circuits session.

In the demonstration the measurement setup, alignment process of the recorded traces and signatures at the IVR input for different modes of the IVR will be demonstrated. A portable oscilloscope will be used to display the signatures directly on the monitor. The Arduino will be programmed to go through different modes of the IVR which will demonstrate live the change in input signatures of the IVR as different modes are enabled and disabled. The TVLA results for different filter bands at the IVR input will be demonstrated. This will be accompanied by a poster to explain the design of the testchip. The chip is driven by USB powered LDOs on the PCB.

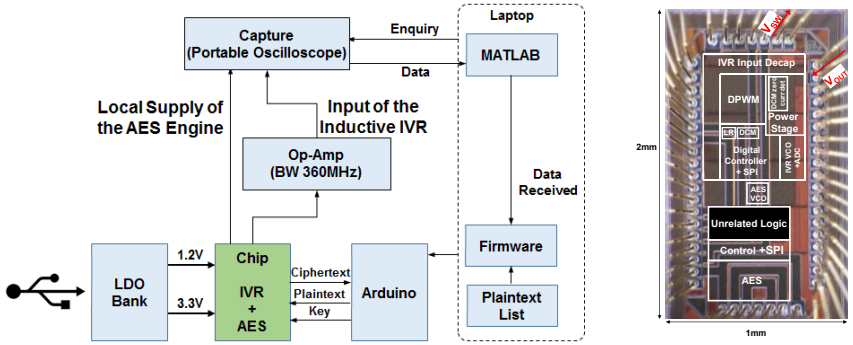

Fig 1. (Left) Test setup. (Right) Micrograph of the fabricated die.